IN THE CLAIMS:

Please amend the claims as indicated. A complete set of the claims is included below, reflecting added subject matter (*underlining)* and deleted subject matter *(strikethrough)*, as well as the current status of each claim. This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Canceled)

22. (Previously Presented) A method of processing a query comprising:
a) accessing said query comprising user identification data, said query further comprising an unencrypted portion comprising unencrypted data and an encrypted portion comprising an encrypted buffer encrypted using a first encryption key, said encrypted buffer also encrypted using a second encryption key;
b) obtaining said second encryption key;
c) decrypting at least a portion of said encrypted portion using said second encryption key;
d) decrypting said encrypted buffer using said first encryption key;
e) determining authentication by comparing said user identification data to user identification data contained within said encrypted buffer; and
f) determining authorization to use a service requested in the query based on information indicating services accessible by the user contained within said encrypted buffer if the user identification data matches user identification data contained within said encrypted buffer.

23. (Canceled)

24. (Previously Presented) A method as described in Claim 22 wherein said b) obtaining said second encryption key comprises determining said second encryption key using at least a portion of said unencrypted data of said query.

25. (Previously Presented) A method of processing a query comprising:

a) accessing said query comprising user identification data, said query further comprising an unencrypted portion comprising unencrypted data and an encrypted portion comprising an encrypted buffer encrypted using a first encryption key, said encrypted buffer also encrypted using a second encryption key;

b) obtaining said second encryption key;

c) decrypting at least a portion of said encrypted portion using said second encryption key;

d) decrypting said encrypted buffer using said first encryption key; and

e) determining authentication by comparing said user identification data to user identification data contained within said encrypted buffer;

wherein said query further comprises a request buffer encrypted using said second encryption key and wherein said request buffer is decrypted at said c) and further comprising transmitting said unencrypted request buffer to a site providing service related to said query provided said query is determined to be authentic and authorized.

26. (Previously Presented) A method as recited in Claim 25 further comprising:

receiving a response from said site; and

forwarding said response.

27. (Previously Presented) A method as recited in Claim 26 wherein said forwarding further comprises:

encrypting said response; and

forwarding said response.

28. (Previously Presented) A method as recited in Claim 24 wherein said second encryption key is determined using a hash of at least three elements.

29. (Previously Presented) A method as recited in Claim 28 wherein said second encryption key is determined by a MD-5 hash of said user identification data, a randomly generated number and a third encryption key.

30. (Previously Presented) A method as recited in Claim 28 wherein said second encryption key is determined by a MD-5 hash of said user identification data, a randomly generated number and said first encryption key.

31. (Previously Presented) A computer system comprising:

a processor coupled to a bus;

a memory unit coupled to said bus and comprising instructions that when executed by said processor implement a method of processing queries comprising:

a) accessing a query comprising user identification data, said query further comprising an unencrypted portion comprising unencrypted data and an encrypted portion comprising an encrypted buffer encrypted using a first encryption key, said encrypted buffer encrypted using a second encryption key;

b) obtaining said second encryption key;

c) decrypting at least a portion of said encrypted portion of said query using said second encryption key;

d) decrypting said encrypted buffer using said first encryption key;

e) determining authentication by comparing said user identification data to user identification data contained within said encrypted buffer; and

f) determining authorization to use a service requested in the query based on information indicating services accessible by the user contained within said encrypted buffer if the user identification data matches user identification data contained within said encrypted buffer.

32. (Canceled)

33. (Previously Presented) A system as described in Claim 31 wherein said b) obtaining said second encryption key comprises determining said second encryption key using at least a portion of said unencrypted data of said query.

34. (Previously Presented) A computer system comprising:

a processor coupled to a bus;

a memory unit coupled to said bus and comprising instructions that when executed by said processor implement a method of processing queries comprising:

a) accessing a query comprising user identification data, said query further comprising an unencrypted portion comprising unencrypted data and an encrypted portion comprising an encrypted buffer encrypted using a first encryption key, said encrypted buffer encrypted using a second encryption key;

b) obtaining said second encryption key;

c) decrypting at least a portion of said encrypted portion of said query using said second encryption key;

d) decrypting said encrypted buffer using said first encryption key; and

e) determining authentication by comparing said user identification data to user identification data contained within said encrypted buffer;

wherein said query further comprises a request buffer encrypted using said second encryption key and wherein said request buffer is decrypted at said c) and wherein said method further comprises transmitting said unencrypted request buffer to a site providing service related to said query provided said query is determined to be authentic and authorized.

35. (Previously Presented) A system as recited in Claim 34 wherein said method further comprises:

receiving a response from said site; and

forwarding said response.

36. (Previously Presented) A system as recited in Claim 35 wherein said forwarding further comprises:

encrypting said response; and

forwarding said response.

37. (Previously Presented) A system as recited in Claim 33 wherein said second encryption key is determined using a hash of at least three elements.

38. (Previously Presented) A system as recited in Claim 37 wherein said second encryption key is determined by a MD-5 hash of said user identification data, a randomly generated number and a third encryption key.

39. (Previously Presented) A system as recited in Claim 37 wherein said second encryption key is determined by a MD-5 hash of said user identification data, a randomly generated number and said first encryption key.

40. (Previously Presented) An apparatus for processing a query comprising:

means for accessing said query wherein said query comprises user identification data, said query further comprising an unencrypted portion comprising unencrypted data and an encrypted portion comprising an encrypted buffer encrypted using a first encryption key, said encrypted buffer also encrypted using a second encryption key;

means for obtaining said second encryption key;

means for decrypting at least a portion of said encrypted portion using said second encryption key;

means for decrypting said encrypted buffer using said first encryption key;

means for determining authentication by comparing said user identification data to user identification data contained within said encrypted buffer; and

means for determining authorization to use a service requested in the query based on information indicating services accessible by the user contained within said encrypted buffer if the user identification data matches user identification data contained within said encrypted buffer.

41. (Canceled)

42. (Previously Presented) An apparatus as described in Claim 40 wherein said means for obtaining comprises means for determining said second encryption key using at least a portion of said unencrypted data of said query.

43. (Previously Presented) An apparatus for processing a query comprising:

means for accessing said query wherein said query comprises user identification data, said query further comprising an unencrypted portion comprising unencrypted data and an encrypted portion comprising an encrypted buffer encrypted using a first encryption key, said encrypted buffer also encrypted using a second encryption key;

means for obtaining said second encryption key;

means for decrypting at least a portion of said encrypted portion using said second encryption key;

means for decrypting said encrypted buffer using said first encryption key; and

means for determining authentication by comparing said user identification data to user identification data contained within said encrypted buffer;

wherein said query further comprises a request buffer encrypted using said second encryption key and further comprising means for transmitting said unencrypted request buffer to a site providing service related to said query provided said query is determined to be authentic and authorized.

44. (Previously Presented) An apparatus as recited in Claim 43 further comprising:
means for receiving a response from said site; and
means for forwarding said response.

45. (Previously Presented) An apparatus as recited in Claim 44 wherein said means for forwarding further comprises:
means for encrypting said response.

46. (Previously Presented) An apparatus as recited in Claim 42 wherein said second encryption key is determined using a hash of at least three elements.

47. (Previously Presented) An apparatus as recited in Claim 46 wherein said second encryption key is determined by a MD-5 hash of said user identification data, a randomly generated number and a third encryption key.

48. (Previously Presented) An apparatus as recited in Claim 46 wherein said second encryption key is determined by a MD-5 hash of said user identification data, a randomly generated number and said first encryption key.